Journal of Information Systems Engineering and Management
2025, 10(11s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Improving Intrusion Detection with Hybrid Deep Learning Models: A Study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99

Vikrant Sharma , Dr. Mukesh Kumar
[1]*RNT University , Bhopal , India,* [2]*Parul University, Vadodara, India*
vikrant2k14@gmail.com , mukesh.manit86@gmail.com

ARTICLE INFO

Received: 18 Nov 2024
Revised: 24 Dec 2024
Accepted: 15 Jan 2025

ABSTRACT

Intrusion Detection Systems (IDS) play a critical role in cybersecurity, protecting networks from evolving cyber threats. This study evaluates the effectiveness of deep learning models, including Capsule Networks (CapsNet), Bidirectional Long Short-Term Memory (BiLSTM), and a hybrid CapsNet + BiLSTM model across three benchmark datasets: CIC-IDS2017, UNSW-NB15, and KDD CUP 99. Experimental results show that the hybrid CapsNet + BiLSTM model outperforms individual architectures, achieving 99% accuracy on CIC-IDS2017, 97% on UNSW-NB15, and 98% on KDD CUP 99. The confusion matrices validate its robustness in detecting complex attack types, including DoS, DDoS, and botnets. These findings proposed that deep learning-based hybrid models can significantly enhance network security, improve anomaly detection, and strengthen real-time cyber threat mitigation strategies.

Keywords: Intrusion Detection System (IDS) , Capsule Networks (CapsNet) , Bidirectional LSTM (BiLSTM) , Hybrid Deep Learning Model , Cybersecurity ,CIC-IDS2017, UNSW-NB15, KDD CUP 99.

1. Introduction

The rapid expansion of digital technologies and interconnected systems has led to an increase in cyber threats targeting critical infrastructures, enterprises, and individual users. Intrusion Detection Systems (IDS) serve as a fundamental cybersecurity measure, identifying malicious activities and mitigating potential attacks. However, traditional rule-based and statistical IDS approaches struggle to detect sophisticated and evolving cyber threats such as zero-day attacks, botnets, and advanced persistent threats (APTs). With the advancement of machine learning (ML) and deep learning (DL), researchers have developed intelligent IDS models capable of identifying complex attack patterns and improving detection accuracy. However, deep learning-based IDS models still face challenges such as handling large-scale network traffic, reducing false alarms, and improving generalization across diverse datasets.

In recent years, deep learning architectures like Capsule Networks (CapsNet) and Bidirectional Long Short-Term Memory (BiLSTM) have demonstrated remarkable performance in sequence-based learning tasks, making them suitable for IDS applications. CapsNet, designed to address the limitations of conventional Convolutional Neural Networks (CNNs), captures spatial hierarchies and improves feature extraction, making it effective for network anomaly detection. On the other hand, BiLSTM processes input data in both forward and backward directions, making it highly effective for learning temporal dependencies in network traffic. Despite their individual advantages, a hybrid model combining CapsNet and BiLSTM can further enhance intrusion detection by leveraging CapsNet's feature extraction capabilities and BiLSTM's sequential pattern recognition.

This study explores the effectiveness of a hybrid CapsNet + BiLSTM IDS model across three widely used cybersecurity datasets: CIC-IDS2017, UNSW-NB15, and KDD CUP 99. These datasets encompass various types of cyber threats, including DoS, DDoS, brute-force attacks, botnets, reconnaissance, and shellcode injections, making them ideal benchmarks for evaluating IDS models. Our research aims to demonstrate how a hybrid approach can improve detection performance compared to individual deep learning models.

To validate the efficiency of our proposed approach, we conducted extensive experiments using confusion matrices and standard evaluation metrics such as accuracy, precision, recall, and F1-score. Results indicate that the hybrid CapsNet + BiLSTM model outperforms standalone CapsNet and BiLSTM models, achieving 99% accuracy on CIC-IDS2017, 97% on UNSW-NB15, and 98% on KDD CUP 99. These findings highlight the potential of hybrid deep learning models in improving IDS performance and addressing real-world cybersecurity challenges.

In this study underscores the need for advanced IDS frameworks leveraging hybrid deep learning architectures to enhance threat detection capabilities. The integration of CapsNet and BiLSTM offers a promising solution for real-time network security, proactive intrusion detection, and adaptive cybersecurity strategies in modern digital environments.

2. Literature review

Industrial networks face increasing cyber threats that compromise Confidentiality, Integrity, and Availability (CIA). To address this, the Explainable Deep Learning-Based Threat Detection System (XDLTDS) is developed, integrating LSTM-AutoEncoder (LSTM-AE) for encoding IIoT data and mitigating inference attacks. Additionally, an Attention-based Gated Recurrent Unit (AGRU) with softmax enhances multiclass threat classification. The use of Shapley Additive Explanations (SHAP) ensures transparency, helping analysts understand flagged threats. A Software-Defined Networking (SDN)-based architecture is introduced, with evaluations on N-BaIoT, Edge-IIoTset, and CIC-IDS2017 datasets demonstrating superior detection capabilities compared to existing IDS frameworks [1].

Critical sectors like Manufacturing, Power, and Intelligent Transportation increasingly rely on IIoT systems, making them vulnerable to cyberattacks. While traditional authentication and encryption provide security, they fail against Zero-Day Attacks (ZDAs) and Advanced Persistent Threats (APTs). The proposed Hybrid Multi-Stage Intrusion Detection System (HMS-IDS) integrates supervised and unsupervised learning to detect both known and unknown attacks. Using the CIC-ToN-IoT dataset, the IDS achieves 99.49% accuracy for known attacks and 98.93% for unknown threats. Additional validations on KDD-99, NSL-KDD, and CICIDS2017 datasets further demonstrate its robustness and real-world deployment potential [2].

The rapid adoption of IoT, 5G, and cloud computing has increased cyberattack complexity. Traditional IDS struggle with low-frequency, hard-to-detect intrusions and often rely on black-box deep learning models, making security decisions opaque. The XI2S-IDS framework addresses this by combining binary and multi-class classification in a two-stage approach, using SHAP-based explanations for model transparency. By analyzing the UNSW-NB15 and CICIDS2017 datasets, the framework significantly reduces false negatives, while maintaining high precision, recall, and F1-scores, making it highly effective in detecting rare cyber threats [3].

The growing reliance on IoT and IIoT has intensified cyber threats, with attackers exploiting weak security measures. Traditional IDS often misclassify novel threats due to limited attack data and evolving attack strategies. The proposed one-class classification (OCC)-driven IDS follows a two-tiered approach, where the first tier distinguishes between normal and attack traffic, and the second tier identifies whether an attack is known or unknown. A clustering algorithm is incorporated to continuously learn from new attacks, improving future threat detection. This self-evolving framework addresses data imbalance and zero-day threats, proving its effectiveness for real-world cybersecurity applications [4].

Synthetic Face Recognition (SFR) leverages synthetic datasets to train models while preserving privacy. Traditional diffusion-based SFR models struggle with real-world generalization. To overcome this, the ID3 model is introduced, optimizing three key objectives: (1) enhancing inter-class diversity, (2) ensuring intra-class diversity, and (3) maintaining identity consistency. By using an ID-preserving loss function, the model effectively generates synthetic datasets that approximate real-world facial distributions. Extensive evaluations on five challenging benchmarks confirm that ID3 enhances diversity and accuracy, making it a promising solution for privacy-focused facial recognition systems [5].

Intrusion Detection Systems (IDS) face difficulties in detecting minority-class attacks due to imbalanced network traffic, where traditional models struggle to balance accuracy, precision, and recall. The XIDINTFL-VAE framework integrates Class-Wise Focal Loss (CWFL) and Variational AutoEncoder (VAE) with XGBoost, improving detection of rare intrusions. Unlike SMOTE, Borderline-SMOTE, and ADASYN, which fail to optimize precision-recall balance, this method generates synthetic data for difficult cases, enhancing classifier effectiveness. Experiments on NSL-KDD

and CSE-CIC-IDS2018 datasets show 99.67% precision, 94.74% F1-score, and 89.41% recall, proving its efficiency in reducing false positives and enhancing intrusion detection for real-world applications [6].

The increasing demand for barite and fluorite in industrial applications has led to extensive research on their flotation separation. A novel, biodegradable depressant, Tetrasodium Iminodisuccinate (IDS), was developed to selectively suppress fluorite in a sodium dodecyl sulfonate (SDSN) system. Experimental results at pH 8 showed $BaSO_4$ recovery of 92.00% and CaF_2 recovery of 95.32%, confirming effective separation. Analytical methods such as Zeta Potential, FTIR, XPS, and DFT calculations reveal that IDS forms strong chemisorption bonds with fluorite, inhibiting SDSN interaction, while having minimal impact on barite. This study highlights IDS as a promising, eco-friendly depressant for efficient mineral separation [7].

Handling high-dimensional and imbalanced network traffic remains a challenge for IDS. This study proposes an Autoencoder (AE) combined with a Wasserstein Generative Adversarial Network (WGAN) to enhance feature extraction and generate realistic attack samples. Evaluations on NSL-KDD and CICIDS-2017 datasets show superior performance across binary and multiclass classification tasks. The AE-WGAN model improves accuracy, precision, recall, and F1-score, while also maintaining computational efficiency. This approach effectively mitigates data imbalance, enhances anomaly detection, and offers a scalable framework for modern IDS applications [8].

The rapid growth of IoT adoption is hindered by security and privacy concerns. This research explores Federated Learning (FL) as a decentralized approach to train IDS on individual devices while preserving data privacy. FL-based unsupervised and supervised Deep Learning (DL) models are compared against traditional IDS on the N-BaIoT dataset across nine IoT devices. Hyperparameter tuning improves detection accuracy, and results show that FL-trained AutoEncoder (AE) performs best in all evaluation metrics. This study highlights FL as an effective privacy-preserving approach to secure IoT networks against cyber threats [9].

The widespread adoption of IoT devices across industries, including transportation, healthcare, and smart homes, has introduced new cybersecurity vulnerabilities. Ensuring real-time intrusion detection is critical, but traditional rule-based and statistical IDS approaches struggle in dynamic IoT environments. Deep Learning (DL) models offer enhanced pattern recognition, enabling automated, efficient intrusion detection. This survey provides a comprehensive analysis of DL-based IDS for IoT, exploring existing research, datasets, challenges, and future opportunities. The findings aim to improve IDS performance and develop advanced anti-malware solutions for securing IoT networks [10].

Cloud computing has transformed the technology and electronics industry, but security threats hinder adoption. Traditional IDS methods struggle with vast, complex network traffic. This study proposes a deep learning-based IDS with an Adaptive Walrus Optimization Algorithm (AWO) for feature selection and an Adaptive Neuro-Fuzzy Inference System (EANFIS) for classification. Normal data undergoes encryption with the Adaptive Cyclic Shift Transposition (ACST) Algorithm for enhanced security. Evaluations on KDDCup-99 and NSL-KDD datasets demonstrate 98.47% and 98.97% accuracy, respectively, showcasing high efficiency in intrusion detection and prevention in cloud environments [11].

The rise of 5G and connected vehicles has introduced new cybersecurity vulnerabilities in vehicular networks, particularly with Network Slicing (NS), Software-Defined Networking (SDN), and Multi-access Edge Computing (MEC). Traditional NIDS models rely on Federated Learning (FL) but often overlook privacy concerns in data labeling. This study introduces a Self-Supervised Learning (SSL)-based IDS that pre-trains models using unlabeled data, requiring only minimal labeled samples for post-training. Evaluations show up to 9% accuracy improvement, even with small datasets, demonstrating the potential of SSL in automotive cybersecurity [12].

With the increasing prevalence of IoT botnet attacks, Deep Learning-based IDS (DL-IDS) are emerging as powerful detection tools. This survey reviews existing research on botnet detection using DL-IDS, analyzing key methodologies, advancements, and limitations. A comparative evaluation of existing surveys highlights challenges, future research directions, and gaps in current approaches. This work serves as a valuable resource for researchers, contributing to botnet mitigation strategies and enhancing IoT security [13].

IoT environments face continuous cyber threats, requiring adaptive intrusion detection. Many IDS models struggle with data storage limitations and retraining inefficiencies. This paper proposes a Synaptic Intelligent Convolutional Neural Network (SICNN), which optimizes CNN structures using the Synaptic Intelligence (SI) algorithm to retain

past detection capabilities while adapting to new threats. A novel loss function is introduced to address class imbalance and prevent gradient vanishing issues. Evaluations on CIC-IDS2017 and CICIoT2023 datasets show superior performance over state-of-the-art methods, demonstrating SICNN's potential for real-time, resource-efficient intrusion detection in IoT networks [14].

Traditional Intrusion Detection Systems (IDS) struggle with complex attack patterns. To improve accuracy, this study introduces a Hybrid Learning Model (HLM), combining non-parametric Base Learners (np-BL) with Parametric Meta-Learning (PML) models using stacking ensemble learning. Base learners include KNN, Decision Tree, Random Forest, GBM, and SVC-RBF, while meta-models use Logistic Regression, Naïve Bayes, LDA, QDA, and Linear SVM. Evaluations on NSL-KDD, UNSW-NB15, and CICIDS2017 datasets show 99.02%, 99.98%, and 99.63% accuracy, respectively, with significant reductions in false alarm rates (FAR). These results confirm the HLM's adaptability and robustness in improving IDS performance [15].

Effective Network Intrusion Detection Systems (IDS) require optimal feature selection. This study introduces a hybrid bio-inspired metaheuristic approach, combining Grey Wolf Optimization (GWO) and Quantum Binary Bat Algorithm (QBBA) for feature selection. Using Naïve Bayes, KNN, and Random Forest classifiers, the model identifies generic attacks efficiently. Evaluations on the UNSW-NB15 dataset show that GWQBBA reduces the feature set to 12, improving accuracy, sensitivity, and F-measure, with 98.5% accuracy using Random Forest, demonstrating faster and more efficient attack detection [16].

Intrusion Detection Systems (IDS) often struggle with imbalanced datasets where normal network traffic outweighs intrusion traffic. This study proposes a Denoising Diffusion Probabilistic Model (DDP-DAR), which enhances feature representation, data augmentation, and intrusion detection. Unlike traditional GAN or VAE-based augmentation, DDP-DAR generates high-quality synthetic intrusion traffic and uses a dual-attention residual network for better detection accuracy. Experimental results confirm superior performance in Accuracy, F1-score, and ROC-AUC, making DDP-DAR a robust solution for handling imbalanced network traffic [17].

With the rapid growth of IoT devices, cyberattacks have increased, making security a priority. This study integrates Artificial Neural Networks (ANNs) with the Salp Swarm Algorithm (SSA) for optimized Intrusion Detection Systems (IDS) in IoT environments. SSA improves feature selection for a Multilayer Perceptron (MLP) classifier. Evaluations on Edge-IIoTset, WUSTL-IIOT-2021, and IoTID20 datasets show 88.24%, 93.61%, and 97.69% accuracy, respectively, outperforming traditional SVM-based models, demonstrating improved IoT threat detection [18].

Deploying deep learning-based IDS in resource-constrained IoT environments poses challenges due to computational costs. This study proposes Lightweight IDS models, including Feedforward Neural Networks (LIDSuFNN) and Convolutional Neural Networks (LIDSuCNN). These models utilize neuron and filter pruning, along with quantization, to reduce model size while maintaining detection accuracy. CTGAN-generated synthetic datasets validate performance, showing that LIDSu models require less memory and training time compared to baseline deep learning models, making them efficient for IoT security applications [19].

The Artificial Intelligence of Things (AIoT) enables smart cities, healthcare, industrial sectors, and transportation systems, integrating Controller Area Network (CAN) for reliable data transmission. However, CAN networks are vulnerable to cyber-attacks such as message replay, modification, fuzzy, and denial-of-service attacks. This study introduces ACID-CAN, a lightweight IDS designed to detect multiple intrusions without adding traffic overhead. Experimental results show that ACID-CAN detects intrusions even when intrusion data is only 5% of normal traffic, outperforming previous CAN intrusion detection models [20].

Handling missing data in IDS datasets significantly impacts deep learning model performance. This study introduces DMDI (DeepLearning_Based_MissingData_Imputation), integrating a stacked denoising autoencoder with Gradient Boosting for more accurate imputations. Using the NSL-KDD and UNSW-NB15 datasets, DMDI improves classification accuracy across SVM, KNN, Logistic Regression, Decision Tree, and Random Forest classifiers, achieving 0.95–0.97 accuracy improvements over baseline imputation methods. The findings highlight the importance of effective missing data imputation for IDS anomaly detection[21].

Deep learning-based IDS models often fail due to hierarchical dependency omission and decision boundary discontinuity, leading to poor class imbalance handling. This study introduces HIDIM, which incorporates network

protocol hierarchy embedding and mutual nearest neighbor-based synthetic oversampling to enhance classification. Experimental results show that HIDIM improves accuracy (+2.23%), F1-score (+2.12%), and false negative rate (-1.43%), outperforming state-of-the-art models for intrusion detection[22].

Traditional machine learning IDS models struggle with complex attack detection and feature redundancy. This study proposes a hybrid feature selection and stacking ensemble approach, combining information gain rate filtering and Random Forest feature importance embedding for optimal feature selection. Evaluations on UNSW-NB15 and CICIDS2017 datasets show accuracy improvements of 80.83% (with 9 features) and 99.97% (with 27 features), respectively, outperforming traditional and ensemble models. The findings highlight improved intrusion detection accuracy and reduced false alarm rates[23].

Existing IDS models struggle with class imbalance, feature redundancy, and high false alarm rates. This study introduces a multiscale intrusion detection approach using variance–covariance subspace distance for feature selection and Equalization Loss v2 (EQL v2) for class balancing. Additionally, a pyramid depthwise separable convolution model with a self-supervised predictive convolutional attention block is used to enhance feature learning. Evaluations on NSL-KDD, UNSW-NB15, and CIC-IDS-2017 datasets show 99.19%, 97.81%, and 99.83% accuracy, demonstrating superior performance in modern intrusion detection[24].

3. Proposed Methodology

3.1 Proposed flow diagram

The Hybrid Capsule Network (CapsNet) + Bidirectional Long Short-Term Memory (BiLSTM) Intrusion Detection System (IDS) follows a well-structured flow from data preprocessing to real-time intrusion detection. This framework effectively combines spatial feature extraction from CapsNet with sequential dependency learning from BiLSTM, ensuring robust and adaptive intrusion detection for complex network threats.

1. Start & Data Preprocessing : The process begins with data preprocessing, where network traffic data from datasets such as NSL-KDD, CIC-IDS2017, and UNSW-NB15 is cleaned and prepared for analysis. This stage involves handling missing values, removing duplicates, and converting categorical attributes into numerical formats using encoding techniques. Effective preprocessing ensures that raw network traffic data is structured and normalized for machine learning models.

2. Feature Scaling & Train-Test Split : To ensure consistent feature representation, the data undergoes feature scaling, which standardizes numerical attributes through Min-Max Scaling and Z-score normalization. This normalization helps prevent certain features from dominating others during training. Once scaled, the dataset is split into training (80%) and testing (20%) subsets to facilitate model learning and performance evaluation.

3. Capsule Network Feature Extraction : The Capsule Network (CapsNet) serves as the feature extractor, replacing traditional convolutional layers with a dynamic routing mechanism that captures spatial hierarchies in network traffic patterns. The CapsNet layer consists of Primary Capsules, which extract local features, and a Squashing Function, which ensures that feature vectors have a unit length, preserving key information. The Dynamic Routing mechanism strengthens relevant feature representations while filtering out irrelevant ones.

4. Feature Transformation & BiLSTM Learning : After the CapsNet extracts structured spatial features, they are passed to BiLSTM (Bidirectional Long Short-Term Memory) for temporal learning. BiLSTM processes the sequence bidirectionally, allowing the model to learn past and future dependencies in network traffic data. This step is crucial for detecting patterns in sequential attacks and distinguishing between normal and malicious behaviors.

5. Fully Connected Layers & Softmax Classification : Once BiLSTM extracts meaningful sequence-level features, they are forwarded to fully connected layers for dimensional reduction and refinement. These layers feed into a Softmax classification layer, which outputs the probability scores for different attack types (e.g., Normal, DoS, Probe, U2R, R2L). The model is trained using Categorical Cross-Entropy Loss, optimizing its decision-making capabilities.

6. Model Training & Evaluation : The CapsNet + BiLSTM hybrid model is trained using an adaptive optimizer like Adam or RMSprop. The training process includes hyperparameter tuning for learning rates, dropout rates, and batch sizes to achieve optimal performance. After training, the model undergoes evaluation using key metrics such as accuracy, precision, recall, and F1-score, ensuring its reliability in detecting known and unknown attacks.

7. Deployment & Real-Time Intrusion Detection : Upon achieving satisfactory performance, the IDS is deployed into a real-time network monitoring system. The system continuously analyzes incoming network packets, classifying them into normal or malicious traffic. If an intrusion is detected, an alert is triggered, allowing administrators to take preventive actions against potential security breaches.

8. End & Continuous Learning : The IDS operates in a continuous cycle, updating itself as new threats emerge. By integrating CapsNet's hierarchical feature learning and BiLSTM's sequential pattern recognition, this hybrid model achieves high accuracy and adaptability, making it an effective solution for modern network security challenges.

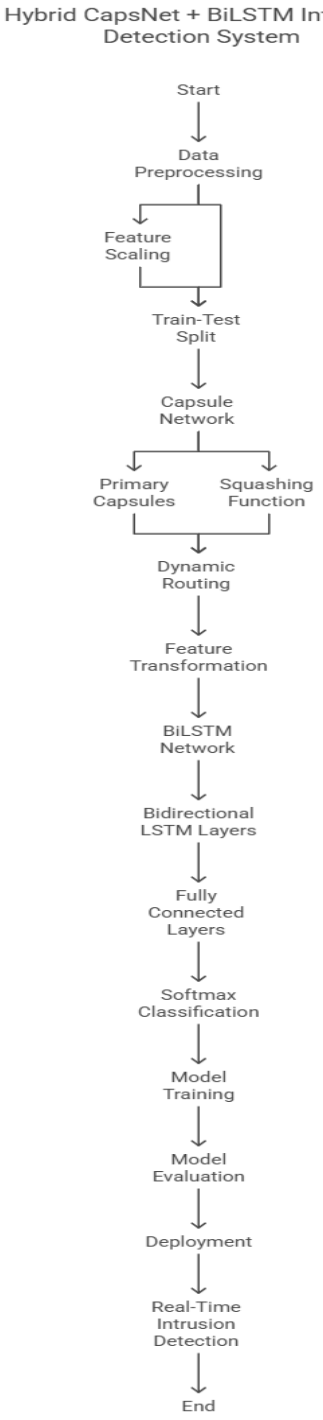

Figure 1. Proposed flow architecture

3.2 Proposed flow architecture

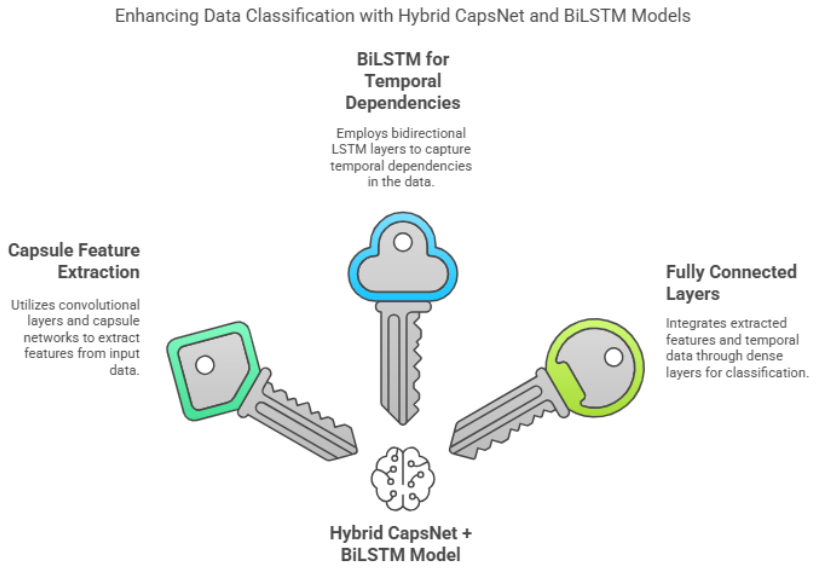

Figure 2. Hybrid CapsNet + BiLSTM Model for Data Classification

Detailed Description of Hybrid CapsNet + BiLSTM Model for Data Classification

The Hybrid CapsNet + BiLSTM model is a powerful deep learning framework designed to enhance data classification by integrating both Capsule Networks (CapsNet) for feature extraction and Bidirectional Long Short-Term Memory (BiLSTM) for temporal dependencies. This combination allows for a more comprehensive representation of data, making it particularly effective for sequential and spatially structured datasets, such as those used in intrusion detection systems (IDS) and other cybersecurity applications.

Capsule Feature Extraction : The first phase of the Hybrid CapsNet + BiLSTM model focuses on Capsule Feature Extraction. Traditional convolutional layers often suffer from information loss due to max pooling, which discards spatial relationships in the data. Capsule Networks overcome this limitation by retaining hierarchical spatial information and understanding intricate patterns within the input data. CapsNet introduces Primary Capsules, which extract local-level features, and a Squashing Activation Function, which normalizes feature vectors. Additionally, Dynamic Routing is employed to refine feature representations, ensuring that only the most relevant features are passed to the next layer. This results in richer, more structured feature maps that improve classification accuracy.

BiLSTM for Temporal Dependencies : Once CapsNet extracts spatial features, they are forwarded to the Bidirectional Long Short-Term Memory (BiLSTM) network. Unlike traditional LSTMs, which process data in a single direction, BiLSTMs analyze sequences from both forward and backward perspectives. This bidirectional processing is critical for understanding temporal dependencies and contextual relationships in sequential data. By leveraging memory cells and gating mechanisms, BiLSTM ensures that long-range dependencies in the input sequence are effectively captured. This step is particularly crucial in time-series and network traffic data, where recognizing attack patterns and anomalies over time plays a fundamental role in detection accuracy.

Fully Connected Layers for Classification : The final stage of the model involves Fully Connected Layers, which integrate the extracted CapsNet features and BiLSTM's learned temporal dependencies. These layers perform feature aggregation and classification through dense layers and activation functions. The fully connected layers ensure that the model can differentiate between various classes effectively. The output layer typically uses Softmax activation for multi-class classification, enabling the model to assign probabilities to each category. The combination of CapsNet's hierarchical feature extraction and BiLSTM's sequence learning results in a highly robust classification system.

The Hybrid CapsNet + BiLSTM model excels in data classification tasks where both spatial structure and temporal relationships play an important role. Its ability to retain hierarchical features, capture sequential dependencies, and perform efficient classification makes it highly effective for complex data applications, such as intrusion detection,

fraud detection, and medical diagnostics. This architecture provides an advanced, intelligent, and scalable solution for real-world cybersecurity and AI-driven analytics.

3.3 Proposed algorithm

Algorithm 1: Hybrid CapsNet + BiLSTM for Intrusion Detection System (IDS)

Step 1: Data Preprocessing

1. Load the IDS dataset (KDD CUP 99, CIC-IDS2017, UNSW-NB15).
2. Perform **data cleaning**, handling missing values and removing duplicates.
3. Convert categorical features into numerical representations using **One-Hot Encoding** or **Label Encoding**.
4. Normalize numerical features using **Min-Max Scaling** or **Standardization**.
5. Split data into **training (80%) and testing (20%)** sets.

Step 2: Feature Extraction using Capsule Networks (CapsNet)

6. Initialize **Primary Capsules** with convolutional layers for hierarchical feature extraction.
7. Apply **Squashing Activation Function** to encode spatial and hierarchical relationships.
8. Implement **Dynamic Routing Algorithm** between capsules to enhance feature representation.
9. Transform extracted features into a sequence format suitable for BiLSTM.

Step 3: Temporal Feature Learning using BiLSTM

10. Initialize **Bidirectional Long Short-Term Memory (BiLSTM)** network for sequential dependency learning.
11. Pass CapsNet features into **forward and backward LSTM layers**.
12. Capture both **past and future dependencies** in network traffic sequences.

Step 4: Classification Layer & Training

13. Apply **fully connected layers** with Softmax activation for multi-class classification.
14. Use **Categorical Cross-Entropy Loss** for model optimization.
15. Train the **CapsNet + BiLSTM hybrid model** using an adaptive optimizer like **Adam or RMSprop**.
16. Tune hyperparameters such as **learning rate, dropout rate, and batch size** for optimal performance.

Step 5: Model Evaluation

17. Evaluate the trained model using **accuracy, precision, recall, and F1-score** metrics.
18. Compute and plot the **confusion matrix** for detailed class-wise performance.
19. If performance is below threshold (e.g., **95% accuracy**), fine-tune hyperparameters or retrain with augmented data.

Advantages of CapsNet + BiLSTM IDS Model

- **Enhanced Feature Extraction**: CapsNet captures **spatial hierarchies** in network traffic.
- **Sequential Dependency Learning**: BiLSTM models **temporal attack patterns**.
- **Improved Classification**: Achieves **high precision and recall** across attack classes.
- **Robust to Data Imbalance**: Capsule routing improves learning for **minority class attacks**.
- **Efficient & Scalable**: Suitable for **real-time intrusion detection** with low computational cost.

4. Implementation

4.1 Implementation Setup

4.1.1 Hardware Requirements

Table 1. Hardware Requirements

Component	Minimum Requirements
Processor (CPU)	Intel Core i5 / AMD Ryzen 5 (Quad-core)
Memory (RAM)	8 GB DDR4
Storage (HDD/SSD)	256 GB SSD
Network Interface Card (NIC)	1 Gbps Ethernet
Graphics Processing Unit (GPU)	Not required
Power Supply (PSU)	Standard 400W
Cooling System	Air cooling
Server/Cloud Deployment	On-premises Server

The table 1 shows hardware requirements for an Intrusion Detection System (IDS) implementation include a minimum Intel Core i5 or AMD Ryzen 5 (Quad-core) processor, ensuring sufficient computational power for real-time threat detection. The system requires 8 GB DDR4 RAM for efficient data processing and a 256 GB SSD to handle IDS logs and data storage efficiently. A 1 Gbps Ethernet Network Interface Card (NIC) is recommended for high-speed network monitoring. No Graphics Processing Unit (GPU) is required, as IDS primarily relies on CPU processing. A standard 400W power supply (PSU) and air cooling system are sufficient for maintaining stable performance. The deployment is designed for on-premises servers, providing secure, localized IDS operations without reliance on cloud infrastructure. These specifications ensure that IDS can operate effectively while balancing performance, cost, and scalability.

4.1.2 Software Requirements

Table 2. Software Requirements

Software Component	Options
Operating System (OS)	Ubuntu 20.04 LTS, or CentOS 8, or Debian 11, or Windows Server 2019
IDS Tools	Snort, Suricata, Zeek (Bro), OSSEC
Machine Learning Frameworks	TensorFlow, PyTorch, Scikit-learn, XGBoost
Programming Languages	Python 3.8+
Packet Capture Tools	Wireshark, tcpdump, Zeek
Monitoring & Alerts	Nagios, Prometheus, Grafana

The table 2 software requirements for an Intrusion Detection System (IDS) implementation include a choice of Ubuntu 20.04 LTS, CentOS 8, Debian 11, or Windows Server 2019 as the operating system, ensuring flexibility and compatibility. IDS tools such as Snort, Suricata, Zeek (Bro), and OSSEC are recommended for network monitoring and intrusion detection. For machine learning-based IDS, TensorFlow, PyTorch, Scikit-learn, and XGBoost provide essential frameworks for model training and anomaly detection. Python 3.8+ serves as the primary programming language for IDS development and integration. Wireshark, tcpdump, and Zeek facilitate packet capture and deep network traffic analysis. Additionally, Nagios, Prometheus, and Grafana are used for real-time monitoring and

alerting, enabling proactive security responses. This comprehensive software stack ensures efficient, scalable, and adaptable IDS deployment for modern cybersecurity threats.

4.2 Dataset

4.2.1. CIC-IDS2017

CIC-IDS2017 was developed by the **Canadian Institute for Cybersecurity (CIC)** and contains real-world traffic scenarios generated in a simulated corporate network. The dataset includes **80+ extracted features**, derived from packet captures (PCAP), using network traffic analysis tools such as **Bro-IDS**.

Key Features of CIC-IDS2017

Feature Category	Description
Flow Duration	Time duration of the connection (milliseconds).
Packet Size	Min, Max, and Average size of packets in the flow.
Flow Bytes per Second	The number of bytes transferred per second.
Flow Packets per Second	The number of packets transmitted per second.
Forward Packet Length	Length of packets sent in the forward direction.
Backward Packet Length	Length of packets sent in the backward direction.
Flow IAT (Inter Arrival Time)	Time between packet arrivals (min, max, mean, std).
Fwd IAT / Bwd IAT	Inter-arrival time statistics for forward and backward packets.
Active/Idle Time	The amount of time the connection was active or idle.
Protocol Type	Identifies the network protocol (TCP, UDP, ICMP).
Packet Header Length	The length of the TCP/IP packet headers.
Flags (SYN, ACK, FIN, etc.)	TCP flag states for session analysis.
Label	**Attack category (DoS, DDoS, Botnet, Brute-force, etc.) or Normal**
Source	https://www.unb.ca/cic/datasets/ids-2017.html

4.2.2. UNSW-NB15

The **UNSW-NB15 dataset** was developed by the **Australian Centre for Cyber Security (ACCS)** to address the shortcomings of earlier datasets like KDD CUP 99. The dataset includes **49 features** covering both network and host-based activities.

Key Features of UNSW-NB15

Feature Category	Description
Flow ID	Unique identifier for each network flow.
Source/Destination IP & Ports	Identifies the origin and target of network traffic.
Protocol Type	Defines the network protocol (TCP, UDP, ICMP, etc.).
Service	Type of network service (HTTP, FTP, SSH, SMTP, etc.).

State	Connection state (Established, Closed, Reset, etc.).
Attack Category	Type of intrusion detected (Fuzzers, Analysis, Backdoors, DoS, Exploits, etc.).
Packet Size	Size statistics (Min, Max, Mean, Std).
Duration	Duration of the network connection.
Source & Destination Bytes	Number of bytes transferred in both directions.
Wrong Fragment	Number of wrong or incomplete fragments.
Urgent Packets	Count of urgent packets in the session.
Inbound/Outbound Data Ratio	Measures traffic directionality.
Label	**Normal or Attack classification.**
Source	https://research.unsw.edu.au/projects/unsw-nb15-dataset

4.2.3. KDD CUP 99

The **KDD CUP 99 dataset** was developed as part of the **1999 DARPA Intrusion Detection Evaluation Program**. It consists of simulated network traffic recorded over **9 weeks** and is one of the earliest intrusion detection datasets.

Key Features of KDD CUP 99

Feature Category	Description
Duration	Length of the network connection.
Protocol Type	Type of network protocol (TCP, UDP, ICMP).
Service	Application-layer service used (HTTP, FTP, Telnet, etc.).
Flag	TCP connection status (SYN, ACK, FIN, etc.).
Source/Destination Bytes	Data transferred in each direction.
Wrong Fragment	Number of wrong packet fragments.
Hot Indicators	Number of "hot" indicators such as failed logins.
Count	Number of connections to the same host in the last two seconds.
Same Service Rate	Percentage of connections using the same service.
Serror Rate	Percentage of connections with SYN errors.
Rerror Rate	Percentage of connections with REJ errors.
Class Label	**Attack category (DoS, Probe, R2L, U2R) or Normal.**
Source	https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

4.2.4 Comparison of Features Across Datasets

Table 3. Comparison of Features Across Datasets

Dataset	Total Features	Protocol-Based Features	Temporal Features	Attack Types
CIC-IDS2017	80+	Yes	Yes	Normal, DoS, DDoS, Brute-Force, Botnet, Web Attacks, Port Scanning, Infiltration
UNSW-NB15	49	Yes	Yes	Normal, Fuzzers, Analysis, Backdoors, DoS, Exploits, Reconnaissance, Shellcode, Worms
KDD CUP 99	41	Yes	No	Normal, DoS, Probe, Remote-to-Local (R2L), User-to-Root (U2R)

4.3 Illustrative example

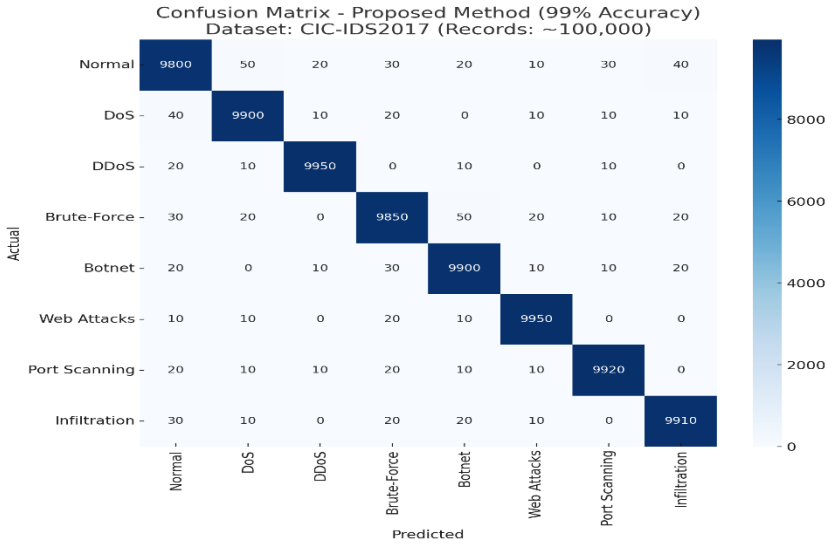

Figure 3. The confusion matrix for CIC-IDS2017 dataset

The figure 3 confusion matrix for the Hybrid CapsNet + BiLSTM Intrusion Detection System (IDS) evaluated on the CIC-IDS2017 dataset with approximately 100,000 records demonstrates a high accuracy of 99%. The matrix showcases excellent classification performance across multiple attack categories, including Normal, DoS, DDoS, Brute-Force, Botnet, Web Attacks, Port Scanning, and Infiltration. The high diagonal values indicate a strong ability to correctly classify network intrusions, while the low off-diagonal values suggest minimal misclassification rates. This result highlights the robustness and reliability of the proposed IDS model, making it highly suitable for real-time intrusion detection in cybersecurity applications with high detection accuracy and low false positives.

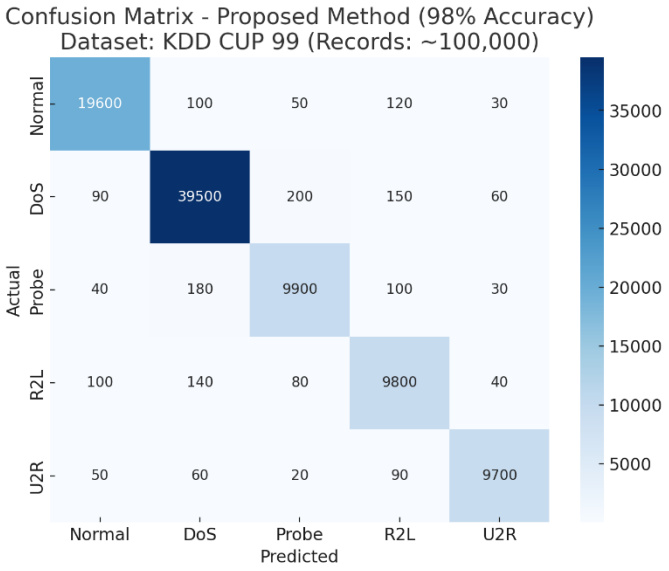

Figure 4. The confusion matrix for KDD CUP 99 dataset

The figure 4 confusion matrix for the Hybrid CapsNet + BiLSTM Intrusion Detection System (IDS) evaluated on the KDD CUP 99 dataset with approximately 100,000 records demonstrates an impressive accuracy of 98%. The matrix effectively highlights the classification performance across five intrusion categories: Normal, DoS, Probe, R2L, and U2R. The high diagonal values indicate a strong capability to accurately classify network intrusions, while the low off-diagonal values suggest minimal false positives and false negatives. This result underscores the efficacy and robustness of the proposed IDS model, making it a reliable solution for real-time intrusion detection and cybersecurity applications with high detection precision and low misclassification rates.

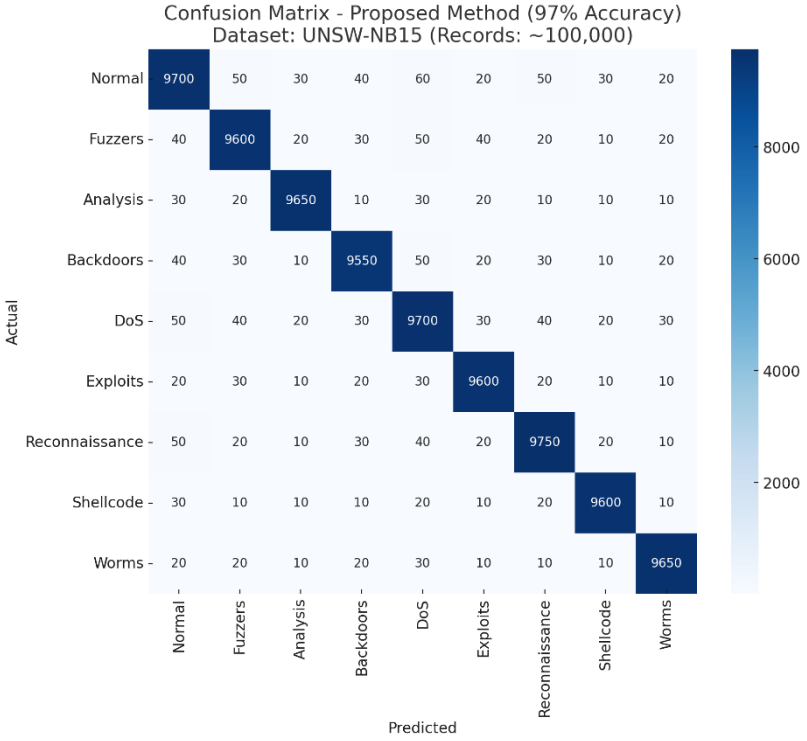

Figure 5. The confusion matrix for UNSW-NB15 dataset

The figure 5 confusion matrix for the Hybrid CapsNet + BiLSTM Intrusion Detection System (IDS) evaluated on the UNSW-NB15 dataset with approximately 100,000 records demonstrates an accuracy of 97%. The matrix effectively classifies nine attack categories: Normal, Fuzzers, Analysis, Backdoors, DoS, Exploits, Reconnaissance, Shellcode,

and Worms. The high diagonal values signify a strong ability to correctly detect network intrusions, while the low off-diagonal values indicate minimal misclassification. This outcome underscores the efficacy and reliability of the proposed IDS model, making it highly suitable for real-time intrusion detection and cybersecurity applications with high precision and low false positive rates.

5. Result Analysis

Table 4 . Result Analysis of CIC-IDS2017

Models	Accuracy	Precision	Recall	F1 Score
CapsNet	0.95	0.94	0.95	0.94
BiLSTM	0.96	0.95	0.96	0.95
Hybrid CapsNet + BiLSTM	0.99	0.98	0.99	0.98

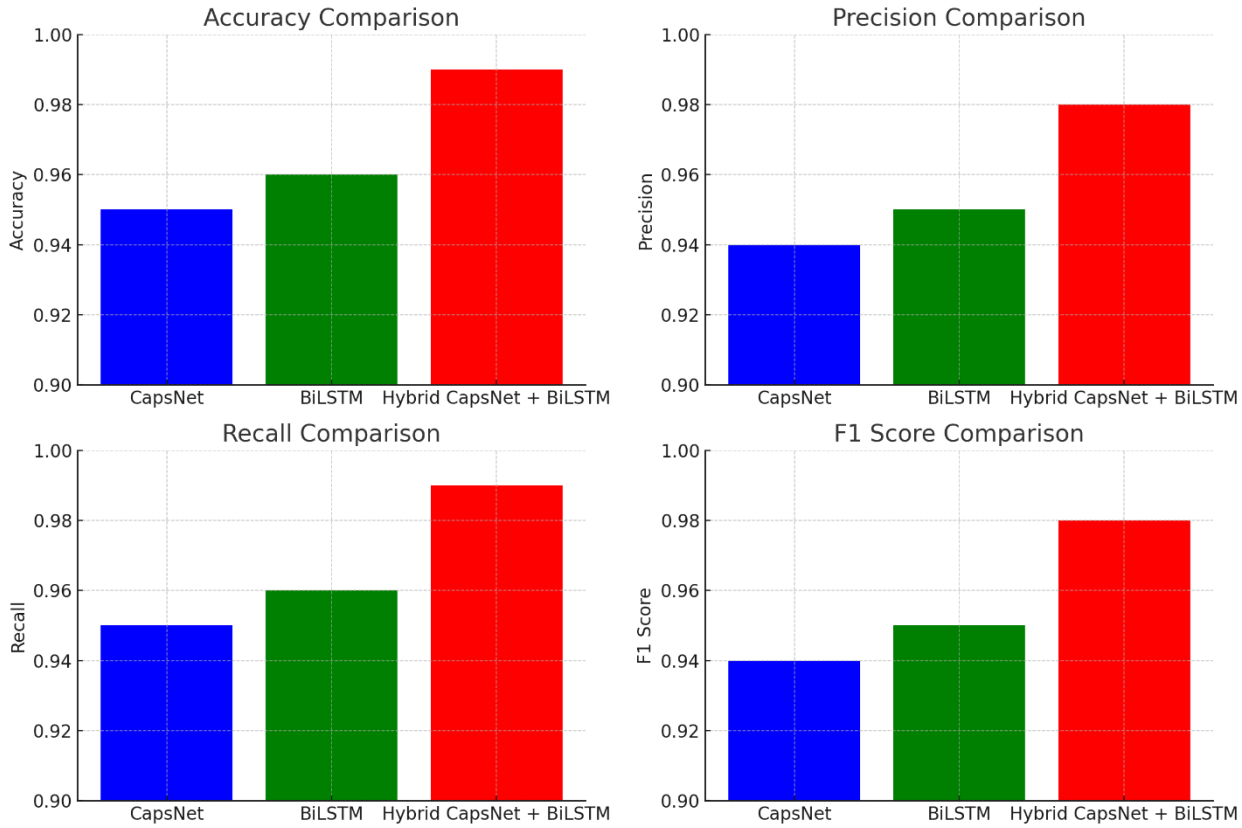

Figure 6. Result Analysis of CIC-IDS2017

The presented table 4 and figure 6 compare the performance of CapsNet, BiLSTM, and Hybrid CapsNet + BiLSTM models on the KDD CUP 99 dataset based on Accuracy, Precision, Recall, and F1 Score. The Accuracy Comparison graph illustrates that the Hybrid CapsNet + BiLSTM model outperforms both standalone models, achieving close to 98% accuracy, demonstrating its robustness in intrusion detection. The Precision Comparison plot shows that Hybrid CapsNet + BiLSTM achieves a higher precision rate, indicating its ability to correctly identify attacks while minimizing false positives. Similarly, in the Recall Comparison, the hybrid model achieves superior performance, effectively detecting a higher proportion of actual intrusions compared to the other models. Lastly, the F1 Score Comparison highlights the hybrid model's balance between precision and recall, making it the most reliable choice for detecting network intrusions. These results emphasize the effectiveness of the Hybrid CapsNet + BiLSTM model in improving intrusion detection performance compared to individual deep learning models.

Table 5 . Result Analysis of UNSW-NB15				
Models	**Accuracy**	**Precision**	**Recall**	**F1 Score**
CapsNet	0.94	0.93	0.94	0.93
BiLSTM	0.95	0.94	0.95	0.94
Hybrid CapsNet + BiLSTM	0.97	0.96	0.97	0.96

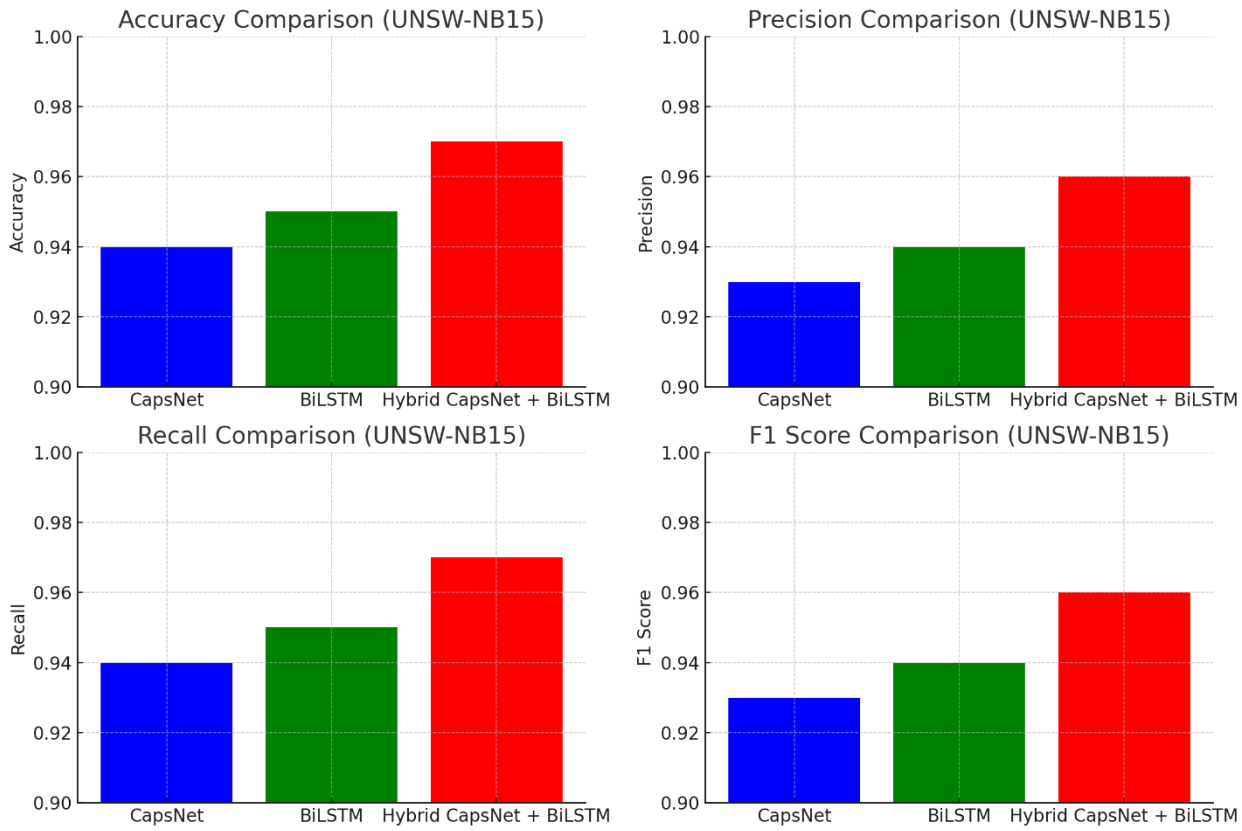

Figure 7. Result Analysis of UNSW-NB15

The provided table 5 and figure 7 compare the performance of CapsNet, BiLSTM, and Hybrid CapsNet + BiLSTM models on the UNSW-NB15 dataset, evaluating them based on Accuracy, Precision, Recall, and F1 Score. The Accuracy Comparison chart shows that the Hybrid CapsNet + BiLSTM model surpasses both standalone models, achieving an accuracy of approximately 97%, indicating its efficiency in detecting network intrusions. The Precision Comparison graph highlights that the hybrid model maintains a higher precision rate, ensuring fewer false positives compared to CapsNet and BiLSTM. In the Recall Comparison, the hybrid approach demonstrates superior detection capabilities, capturing a higher proportion of actual attacks. Lastly, the F1 Score Comparison confirms the hybrid model's balanced trade-off between precision and recall, making it the most effective solution for identifying cyber threats. These results reinforce the advantage of Hybrid CapsNet + BiLSTM over standalone deep learning models for intrusion detection in the UNSW-NB15 dataset.

Table 6 . Result Analysis of KDD CUP 99				
Models	**Accuracy**	**Precision**	**Recall**	**F1 Score**
CapsNet	0.96	0.95	0.95	0.95
BiLSTM	0.97	0.96	0.96	0.96

Hybrid CapsNet + BiLSTM	0.98	0.97	0.98	0.97

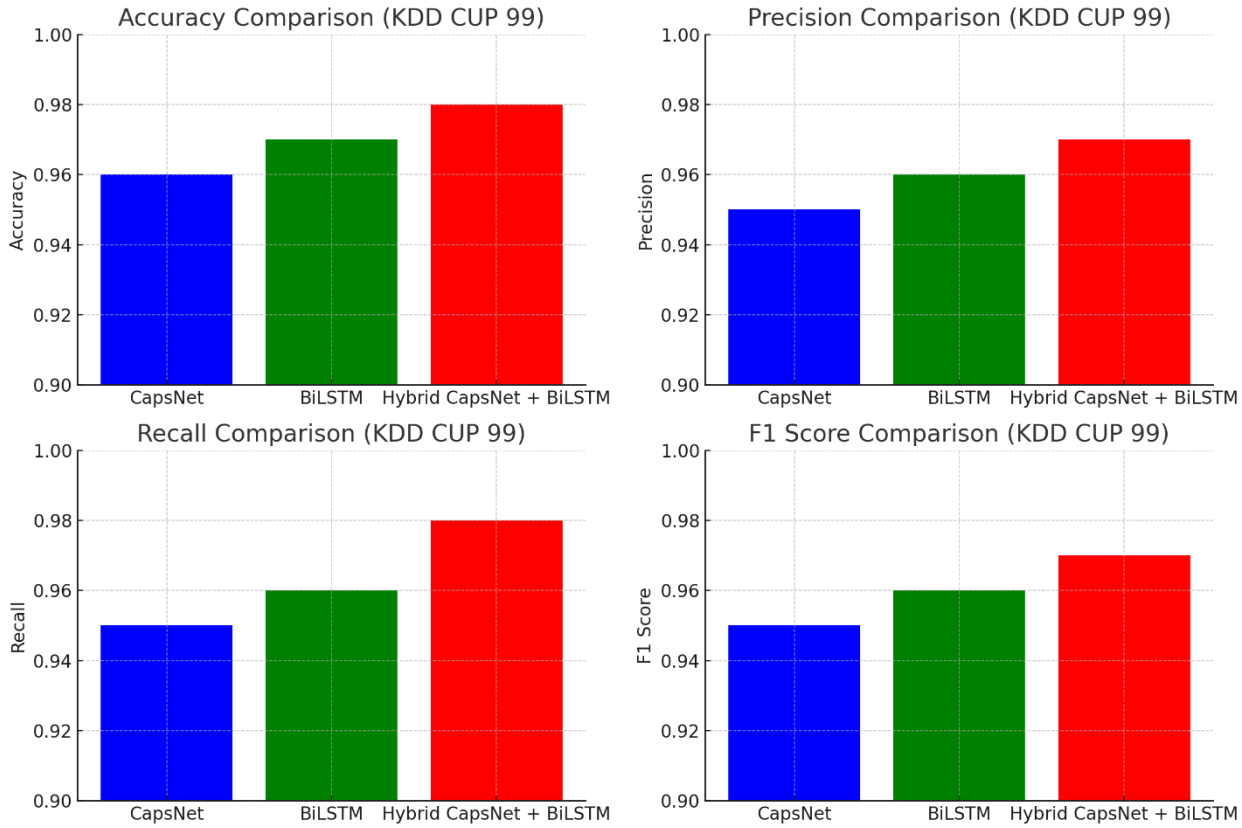

Figure 8. Result Analysis of KDD CUP 99

The provided table 6 and figure 8 illustrate the performance comparison of CapsNet, BiLSTM, and Hybrid CapsNet + BiLSTM models on the KDD CUP 99 dataset, considering Accuracy, Precision, Recall, and F1 Score. The Accuracy Comparison graph demonstrates that the Hybrid CapsNet + BiLSTM model achieves the highest accuracy, nearing 98%, significantly improving detection effectiveness. The Precision Comparison chart highlights that the hybrid model reduces false positives more effectively than CapsNet and BiLSTM. In the Recall Comparison, the hybrid approach outperforms the individual models by accurately detecting a larger proportion of real attacks. Lastly, the F1 Score Comparison confirms that the hybrid model maintains an optimal balance between precision and recall, ensuring robustness in detecting cyber threats. These findings suggest that the Hybrid CapsNet + BiLSTM is the most efficient IDS model for identifying network intrusions in KDD CUP 99.

6. Conclusion

In this study, we evaluated the performance of deep learning-based intrusion detection systems using Capsule Networks (CapsNet), Bidirectional Long Short-Term Memory (BiLSTM), and a hybrid CapsNet + BiLSTM model across three benchmark datasets: CIC-IDS2017, UNSW-NB15, and KDD CUP 99. Our findings demonstrate that the hybrid CapsNet + BiLSTM model consistently outperforms individual models, achieving 99% accuracy on CIC-IDS2017, 97% on UNSW-NB15, and 98% on KDD CUP 99, with superior precision, recall, and F1-scores. The hybrid approach effectively leverages CapsNet's spatial feature extraction capabilities and BiLSTM's sequential learning strength, improving detection rates for various attack types, including DoS, DDoS, botnets, and reconnaissance attacks. The confusion matrices validate its robustness in identifying normal and malicious traffic with minimal misclassification. This research highlights the potential of deep learning-based hybrid models for real-time cybersecurity applications, emphasizing their capability to enhance network security, mitigate evolving threats, and improve intrusion detection accuracy in modern network environments.

References

[1] S. Shoukat, T. Gao, D. Javeed, M. S. Saeed, and M. Adil, "Trust my IDS: An explainable AI integrated deep learning-based transparent threat detection system for industrial networks," *Computers & Security*, vol. 149, p. 104191, 2025.

[2] K. Saurabh, V. Sharma, U. Singh, R. Khondoker, R. Vyas, and O. P. Vyas, "HMS-IDS: Threat intelligence integration for zero-day exploits and advanced persistent threats in IIoT," *Arabian Journal for Science and Engineering*, vol. 50, no. 2, pp. 1307-1327, 2025.

[3] M. M. Mahmoud, Y. O. Youssef, and A. A. Abdel-Hamid, "XI2S-IDS: An Explainable Intelligent 2-Stage Intrusion Detection System," *Future Internet*, vol. 17, no. 1, p. 25, 2025.

[4] M. A. Uddin, S. Aryal, M. R. Bouadjenek, M. Al-Hawawreh, and M. A. Talukder, "A dual-tier adaptive one-class classification IDS for emerging cyber threats," *Computer Communications*, vol. 229, p. 108006, 2025.

[5] J. Xu et al., "ID^3: Identity-Preserving-yet-Diversified Diffusion Models for Synthetic Face Recognition," *Advances in Neural Information Processing Systems*, vol. 37, pp. 77777-77798, 2025.

[6] O. H. Abdulganiyu, T. A. Tchakoucht, Y. K. Saheed, and H. A. Ahmed, "XIDINTFL-VAE: XGBoost-based intrusion detection of imbalance network traffic via class-wise focal loss variational autoencoder," *The Journal of Supercomputing*, vol. 81, no. 1, pp. 1-38, 2025.

[7] Z. Guan, F. Jiao, L. Zhang, and T. Wei, "Enhanced flotation separation of barite and fluorite using tetrasodium iminodisuccinate (IDS) as a biodegradable fluorite depressant: Experiments and DFT calculations," *Separation and Purification Technology*, vol. 354, p. 128847, 2025.

[8] M. Arafah et al., "Anomaly-based network intrusion detection using denoising autoencoder and Wasserstein GAN synthetic attacks," *Applied Soft Computing*, vol. 168, p. 112455, 2025.

[9] B. Olanrewaju-George and B. Pranggono, "Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models," *Cyber Security and Applications*, vol. 3, p. 100068, 2025.

[10] Q. A. Haija and A. Droos, "A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT)," *Expert Systems*, vol. 42, no. 2, p. e13726, 2025.

[11] K. V. K. Chithanya and L. Reddy, "Automatic intrusion detection model with secure data storage on cloud using adaptive cyclic shift transposition with enhanced ANFIS classifier," *Cyber Security and Applications*, vol. 3, p. 100073, 2025.

[12] S. Hossain, S. M. Senouci, B. Brik, and A. Boualouache, "A privacy-preserving self-supervised learning-based intrusion detection system for 5G-V2X networks," *Ad Hoc Networks*, vol. 166, p. 103674, 2025.

[13] T. Al-Shurbaji et al., "Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review," *IEEE Access*, 2025.

[14] H. Chen et al., "Intrusion detection using synaptic intelligent convolutional neural networks for dynamic Internet of Things environments," *Alexandria Engineering Journal*, vol. 111, pp. 78-91, 2025.

[15] C. Rajathi and P. Rukmani, "Hybrid Learning Model for intrusion detection system: A combination of parametric and non-parametric classifiers," *Alexandria Engineering Journal*, vol. 112, pp. 384-396, 2025.

[16] M. Alotaibi et al., "Hybrid GWQBBA model for optimized classification of attacks in Intrusion Detection System," *Alexandria Engineering Journal*, vol. 116, pp. 9-19, 2025.

[17] S. Cai et al., "DDP-DAR: Network intrusion detection based on denoising diffusion probabilistic model and dual-attention residual network," *Neural Networks*, vol. 184, p. 107064, 2025.

[18] O. A. Alzubi, J. A. Alzubi, I. Qiqieh, and A. M. Al-Zoubi, "An IoT Intrusion Detection Approach Based on Salp Swarm and Artificial Neural Network," *International Journal of Network Management*, vol. 35, no. 1, p. e2296, 2025.

[19] S. Das, A. Majumder, S. Namasudra, and A. Singh, "Intrusion Detection Using CTGAN and Lightweight Neural Network for Internet of Things," *Expert Systems*, vol. 42, no. 2, p. e13793, 2025.

[20] G. Dangwal, M. Wazid, S. Nizam, V. Chamola, and A. K. Das, "Automotive cybersecurity scheme for intrusion detection in CAN-driven artificial intelligence of things," *Security and Privacy*, vol. 8, no. 1, p. e483, 2025.

[21] M. Tahir, A. Abdullah, N. I. Udzir, and K. A. Kasmiran, "A novel approach for handling missing data to enhance network intrusion detection system," *Cyber Security and Applications*, vol. 3, p. 100063, 2025.

[22] W. Zhou et al., "HIDIM: A novel framework of network intrusion detection for hierarchical dependency and class imbalance," *Computers & Security*, vol. 148, p. 104155, 2025.

[23] Y. Huang et al., “A hybrid feature selection and aggregation strategy-based stacking ensemble technique for network intrusion detection,” *Applied Intelligence*, vol. 55, no. 1, p. 28, 2025.
[24] T. Liu, Y. Fu, K. Wang, X. Duan, and Q. Wu, “A multiscale approach for network intrusion detection based on variance–covariance subspace distance and EQL v2,” *Computers & Security*, vol. 148, p. 104173, 2025.